УДК: 004.421:37

АЛГОРИТМИ АВТОРИЗАЦІЇ ТА ПЕРСОНІФІКАЦІЇ КОРИСТУВАЧІВ ОСВІТНІХ ОНЛАЙН РЕСУРСІВ

Передерій О.С., Осадчий В.В.
Мелітопольський державний педагогічний університет імені Б. Хмельницького,
м. Мелітополь

По мірі розвитку технологічного комп'ютерного прогресу цінність інформації невпинно зростає. Усі приватні дані зберігаються з використанням комп'ютеру, який, як правило, під'єднаний до глобальної мережі. Можливості глобальної мережі Інтернет відкривають величезні горизонти для онлайн комерції, але створюють потребу в надійніших засобах безпеки для захисту даних від зовнішнього доступу. Останніми роками головним методом персоніфікації користувачів була авторизація за логіном і паролем. Проблеми з безпекою в даному випадку добре відомі: паролі забувають, розголошують їх стороннім особам, зрештою, їх можуть вкрасти. З огляду на це, можна зробити висновок, що стандартні методи персоніфікації застаріли.

Проаналізував можливі методи авторизації, стає зрозумілим, що для доступу до системи потрібно застосовувати такі методи ідентифікації, які не працюють окремо від їх носія. Цій вимозі відповідають біометричні характеристики людського організму. Сучасні біометричні технології дозволяють ідентифікувати особу за фізіологічними і психологічними ознаками [3, с. 91].

Термін "біометрія" позначає вимір деяких фізіологічних властивостей людини. Звичайні методі аутентифікації дуже легко обійти, але ошукати

біометричну систему практично неможливо. Нині в якості вимірюваних параметрів використовують відбитки пальців, специфікації голосу, райдужну оболонку очей, а також зовнішній вигляд людини.

Будь-яка біометрична система дозволяє розпізнавати якийсь шаблон і встановлювати автентичність конкретних фізіологічних або поведінкових характеристик користувача. Біометричну систему можна розділити на два модулі: модуль реєстрації та модуль ідентифікації. Перший відповідає за те, щоб навчити систему ідентифікувати конкретну людину. На етапі реєстрації біометричні датчики сканують необхідні фізіологічні або поведінкові характеристики людини і створюють їх цифрове представлення. Спеціальний модуль обробляє цю інформацію для того, щоб виділити характерні особливості та згенерувати більш компактне і виразне уявлення, яке зветься шаблоном. Шаблон для кожного користувача зберігається в базі даних біометричної системи. Модуль ідентифікації відповідає за розпізнавання людини. На етапі ідентифікації біометричний датчик знімає характеристики людини, яку потрібно ідентифікувати, і перетворює ці характеристики до того ж цифрового формату, в якому зберігається шаблон. Отриманий шаблон порівнюється з збереженим, щоб визначити, чи відповідають ці шаблони один одному [5, с. 304].

Переваги біометричних систем безпеки є очевидними: унікальні людські якості важко підробити, важко залишити фальшивий відбиток пальця за допомогою свого власного або зробити райдужну оболонку свого ока схожою на іншу. На відміну від паперових ідентифікаторів, від пароля або персонального ідентифікаційного номера, біометричні характеристики не можуть бути забуті або втрачені, в силу своєї унікальності

вони використовуються для запобігання крадіжки або шахрайства [3, с. 270].

Біометричні технології можна розділити на дві великі категорії: фізіологічні й психологічні. У першому випадку аналізуються такі ознаки, як риси обличчя, структура ока, параметри пальців (папілярні лінії, рельєф), геометрія долоні. Психологічні характеристики - це голос людини, особливості його підпису, динамічні параметри письма і особливості введення тексту з клавіатури [1, с. 17].

Фізіологічні особливості, такі як, папілярний візерунок пальця, геометрія долоні, модель райдужної оболонки ока - це незмінні фізичні особливості людини. Поведінкові ж характеристики залежать як від керованих дій, так і менш керованих психологічних факторів. Оскільки поведінкові характеристики можуть змінюватися в перебігу життя, зареєстрований біометричний зразок має оновлюватися під час кожного користування. Ідентифікація особи за фізіологічними рисам набагато точніша.

В даний час існує три основних методи розпізнавання обличчя, що розрізняються складністю реалізації та метою застосування: аналіз «відмінних рис»; аналіз на основі «нейронних мереж»; метод «автоматичної обробки зображення обличчя» [3, с.109].

У методі аналізу «відмінних рис» використовуються десятки характерних особливостей різних частин обличчя особи з урахуванням їх відносного розташування. Індивідуальна комбінація цих параметрів визначає особливості кожної конкретної особи. У методі, заснованому на нейронній мережі, використовують алгоритм, який встановлює відповідність особистих унікальних параметрів людини і параметрів шаблону, що знаходиться в базі даних, при цьому застосовується максимально можливе число параметрів. По мірі

порівняння визначаються невідповідності між особою, що перевіряється і шаблоном з бази даних, потім запускається механізм, який за допомогою відповідних вагових коефіцієнтів визначає ступінь відповідності. Метод автоматичної обробки зображення обличчя - найбільш проста технологія, що використовує відстані і відношення відстаней між важливими точками обличчя людини, такими, як очі, кінець носа, куточки рота [2, с. 228].

При ідентифікації за сітківкою ока виміряється кутовий розподіл кровоносних судин на поверхні сітківки щодо сліпої плями ока. Перевірка сітківки відбувається з використанням інфрачервоного світла низької інтенсивності, направленого через зіницю до кровоносних судин на задній стінці ока. До вад таких систем варто віднести те, що вони чутливі до неправильної орієнтації сітківки.

За допомогою алгоритмів ідентифікації по райдужній оболонці очей, необроблені відеозображення ока перетворюються в унікальний ідентифікаційний двійковий потік, отриманий в результаті визначення позиції райдужки, її межі та виконання інших математичних операцій для опису текстури райдужки у вигляді послідовності чергування фаз, схожою на штрих-код. Перевага сканерів для райдужної оболонки ока полягає в тому, що вони не вимагають від користувача зосередження на цілі, так як зразок плям на райдужній оболонці знаходиться на поверхні ока [5, с. 359].

При використанні аутентифікації по долоні, використовують такі параметри, як довжина і ширина пальців, співвідношення розмірів долоні або пальців, товщину долоні. Аутентифікація по долоні має високий коефіцієнт помилкового доступу, тому найчастіше використовується в поєднанні з розпізнаванням відбитків пальців.

Увесь процес ідентифікації за малюнком папілярних ліній займає не більше кількох секунд і не потребує зусиль від тих, хто використовує цю систему доступу. Переваги доступу за відбитком пальця - простота користування, зручність використання і надійність. Дактилоскопія побудована на двох головних аспектах, притаманних папілярному візерунку шкіри пальців і долонь: стабільність малюнка візерунка впродовж всього життя людини; унікальність малюнка, що означає відсутність двох індивідуумів з однаковими дактилоскопічними відбитками. Існує два основних алгоритма порівняння із існуючим в базі шаблоном: за характерними точками і за рельєфом всієї поверхні пальця. У першому випадку виявляються характерні ділянки і запам'ятовується їх взаєморозташування. У другому випадку запам'ятовується весь візерунок в цілому. У сучасних системах використовується також комбінація обох алгоритмів, що дозволяє підвищити рівень надійності системи [1, с. 73].

Підпис - такий же унікальний атрибут людини, як і його фізіологічні характеристики. Одна з перспективних технологій аутентифікації заснована на унікальності біометричних характеристик руху людської руки під час письма. Зазвичай виділяють два способи обробки даних про підписи: просте порівняння із зразком і динамічну верифікацію. Перший вельми ненадійний, оскільки заснований на звичайному порівнянні введеного підпису із тим графічним зразком, що зберігається в базі даних. Через те, що підпис не може бути завжди однаковим, цей метод дає великий відсоток помилок. Спосіб динамічної верифікації вимагає набагато складніших обчислень і дозволяє в реальному часі фіксувати параметри процесу підпису, такі, як швидкість руху руки на різних ділянках, сила тиску і тривалість різних етапів підпису [4, с. 136].

Біометричний підхід, пов'язаний з ідентифікацією голосу, комфортний у використанні. Однак основним і

визначальним недоліком цього підходу є низька точність ідентифікації. Постійно ведуться роботи по підвищенню ефективності систем ідентифікації голосом. Відомі системи аутентифікації, де застосовується метод сумісного аналізу голосу та міміки, бо міміка особи характерна лише їй, як і відбитки пальців.

Отже, у статті було розглянуто існуючі методи авторизації та персоніфікації. Було встановлено, що у наш час в освітній сфері використовується персоніфікація користувачів за логіном та паролем. Як було зазначено, цей метод авторизації є застарілим і дуже ненадійним. Тому у перспективі передбачається створення системи аутентифікації користувачів освітніх онлайн ресурсів. У даній системі буде використовуватися алгоритм аналізу голосового пароля для первинної авторизації користувача. Це дозволить позбутися проблем ручного введення пароля, бо контрольну фразу хоча і можна буде дізнатися, але неможливо підробити, так як основним параметром первинної авторизації буде розпізнавання голосу. Щоб зробити дану систему більш надійною і актуальною, надалі, в процесі роботи, будуть зніматися реперні точки за алгоритмом «нейронних мереж». Це дозволить розпізнавати особистість користувача і його міміку в реальному часі. Актуальністю цього неможливо знехтувати, так як це дозволить навчальним онлайн ресурсам проводити тестування, лекції чи інші педагогічні заходи з упевненістю, що саме даний користувач приймає участь у навчальному або тестувальному процесі. Це дозволить зберігати унікальність аунтентифікації протягом усього часу роботи з онлайн ресурсом. Дана система може стати великим досягненням по відношенню до поточного методу персоніфікації, оскільки дозволить повністю контролювати навчання людини, без можливості підробки особистості навіть після її авторизації.

Література

1. Молдовян Н.А. Проблематика и методы криптографии. / Н.А. Молдовян. — СПб.: СПбГУ, 2008. — 212 с.
2. Петров А.А. Компьютерная безопасность. Криптографические методы защиты / А.А. Петров. — М.: ДМК, 2000. — 445с.
3. Романец Ю.В. Защита информации в современных компьютерных системах. / Ю.В. Романец. — М.: Радио и связь, 2003. — 741 с.
4. Смит Р. Аутентификация: от паролей до открытых ключей. / Р. Смит. — М.: Вильямс, 2002. — 432 с.
5. Шнайер Б. Прикладная криптография. Алгоритмы. / Б. Шнайер. — М. :Триумф, 2002. — 816 с.

Аннотация. В данной статье рассмотрены проблемы аутентификации пользователей и проблемы безопасности, связанные с определением личности. Проанализированы проблемы авторизации по имени и паролю пользователя. Рассмотрены возможные решения данной проблемы. Рассмотрены существующие алгоритмы биометрических систем авторизации. Обоснована необходимость использования биометрических параметров для аутентификации пользователей.

Ключевые слова: безопасность, аутентификация, биометрические параметры.

Анотація. У даній статті розглянуто проблеми аутентифікації користувачів і проблеми безпеки, пов'язані з визначенням особи. Проаналізовано проблеми авторизації за логіном і паролем користувача. Розглянуто можливі вирішення даної проблеми. Розглянуто існуючі алгоритми біометричних систем авторизації. Обґрунтовано необхідність використовувати біометричні параметри для аутентифікації користувачів.

Ключові слова: безпека, аутентифікація, біометричні параметри.

Summary. This article discusses the problem of user authentication and security issues associated with the definition of personality in our time. Explored the problems of authentication by user name and password. Identified the possible solutions to this problem. Considered the existing algorithms for biometric authentication systems. The necessity to use biometrics to authenticate users.

Keywords: security, authentication, biometrics.